

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of

Victoria M. BELLOTTI et al.

Group Art Unit: 2145

Application No.: 09/683,532

Examiner: A. CHOUDHURY

Filed: January 16, 2002

Docket No.: 110143

For: SYSTEMS AND METHODS FOR INTEGRATING ELECTRONIC MAIL AND
DISTRIBUTED NETWORKS INTO A WORKFLOW SYSTEM

REPLY BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following remarks are directed to the new points of argument raised in the
Examiner's Answer dated October 3, 2008.

A. Insufficient Rationale for the Combination Of Kim And Rienhoff

Appellants' arguments in the July 18, 2008 Appeal Brief ("Appeal Brief") in the
rejection of claims 1-22 and 25 under 35 U.S.C. §103(a) over Kim in view of Rienhoff
asserted that the alleged motivation for combining Kim and Rienhoff ("restrict access to
secure content") is improper because Rienhoff fails to recognize that Kim already teaches
restricting access to secure content. Therefore, there would be no reason for the alleged
combination as the alleged result is already achieved.

The Examiner in the Examiner's Answer (pgs. 9-10) merely responds that Kim teaches
how users gain access to the workflow system after the receipt of the email embedded with a
link, and that Rienhoff also teaches how a user gains access to a secure area of a site after

clicking on a link that can be received through an email. Then, the Examiner concludes that users (unauthorized) therefore are able to gain access to a restricted area through the link within the email.

However, the Examiner's Answer fails to consider or address that Kim's system uses a VPN (Virtual Private Network), which is secure and requires a registered user for access (see Appellants' July 13, 2006 Amendment). Thus, Kim achieves the alleged reason for the combination so the rationale for combination is improper. Moreover, this would materially change the operation of Kim, which requires VPN registration for access.

Thus, the Examiners rationale for the combination of Rienhoff with Kim must fail. Accordingly, the Examiner has not established a proper *prima facie* case of obviousness under KSR. Independent claims 1, 10 and 21 and claims dependent therefrom distinguish over Kim and Rienhoff.

B. Rienhoff Does Not Teach Or Suggest The Relied Upon Features

Appellants previously argued that the users in Rienhoff are only permitted access after logging in with a login name and password. In response, the Examiner asserts in the Examiner's Answer (pgs. 9-10) that Rienhoff's login is related to the general registration with a site, which is equivalent to a person being entered into a company's email database after getting hired by the company. Therefore, the Examiner alleges that login does not have to occur when accessing the secured area and is an option in Rienhoff. Appellants respectfully disagree. This is merely the Examiner's opinion, which is inconsistent with the disclosure by Rienhoff.

Rienhoff discloses in paragraph [0106] that the user enters user information into a registration form to establish a login and password for permitting access to a secured area of the web site. As discussed in paragraph [0112], based upon the analysis of the questionnaire

forms that the user submitted, the user is directed to a secured area of the web site. When the user attempts to access the secured area of the web site, the user is first directed to a login web site for logging into the secured area of the web site, as discussed in paragraph [0113]. The user then logs into the secured area of the web site by entering the login name and password used in the registration form, or alternatively, an additionally established login name and password.

Therefore, Rienhoff explicitly discloses that the user must be directed to a login web site for logging in, before he is directed to the secured area of the web site. Accordingly, contrary to the Examiner's statement, one of ordinary skill in the art would not have understood the login procedure in Rienhoff to be optional as alleged. Accordingly, the Examiner's "opinion" is inconsistent with the teachings and improper.

Therefore, the combination fails to teach or provide a reason or rationale to provide each and every feature of independent claims 1, 10 and 21. Namely, the combination does not teach that a link in an email provides access to a second workflow system to a recipient who does not have access. Instead, in both Kim and Rienhoff, only registered secured users may access the site and must go through a login procedure. That is, a recipient without access is not granted access by the email link. Instead, he is directed to a login page, which provides the access to only an authorized recipient.

Accordingly, independent claims 1, 10 and 21 and claims dependent therefrom distinguish over Kim and Rienhoff.

C. Kim Does Not Disclose The Subject Matter Recited In Claims 4, 5, 13 And 14

In response to Appellants' argument that the generating of the automatic random key code described in Kim does not correspond to generating a network address, the Examiner alleges in the Examiner's Answer (pg. 10) that Kim discloses this feature because the random

and pseudo-random generation of data (such as network addresses) is implicitly required in a public key cryptographic system.

Appellants agree that randomly-generated data is required as a public key for a cryptographic system that uses the private and public keys, and that Kim uses a random key code linking to the email in order to protect misusing of the mail. However, Kim does not teach or suggest randomly or pseudo-randomly generating the network address, as recited in claims 4 and 13, or generating the network address based on at least in part on information about at least one of at least the created email message, the recipient, the workflow process and the user, as recited in claims 5 and 14. Although the public key generated by Kim is random, it is not the network address but a key used to decrypt the encrypted information. Accordingly, because each and every feature of these claims is not met by Kim or Rienhoff, claims 4, 5, 13 and 14 distinguish over Kim and Rienhoff.

D. Kim Does Not Disclose The Subject Matter Recited In Claim 21

Regarding the rejection of claim 21, the Examiner asserts in the Examiner's Answer (pg. 11) that Kim discloses selecting the link to access the network address, wherein, in response, the work flow system provides access to the work flow process, because Kim teaches how users gain access to the workflow system after the receipt of the email embedded with a link. However, Kim discloses, on page 4, column 1, lines 50-52, that all users must be authenticated by a unique email address on the user management database. Thus, Kim provides that a user must be authenticated before being given access to the system.

Moreover, Kim and Rienhoff fail to disclose or suggest that the network address is specified to the workflow process and to the email message. The URL embedded to email as discloses in Kim and Rienhoff only indicates a link specified to the intended workflow. The link is not specified to the email message sent to the recipient. That is, if the email message

is sent to another recipient, the embedded URL is the same (maybe with different encryptions).

Accordingly, independent claim 21 distinguishes over Kim and Rienhoff

E. Kim Does Not Disclose The Subject Matter Recited In Claim 25

The Examiner repeatedly alleges that Kim discloses the "excluding generating network addresses that have been embedded in previous email messages created by the system that have not yet been accessed" feature of claim 25 because Kim discloses encrypting the URL within each email, allegedly making the encrypted URL unique, and because the embedding of previous links is avoided (Examiner's Answer, pgs. 11-12).

Appellants respectfully submit that encryption/decryption only transforms data into another form. The encrypted data should be decrypted in the same form as before encrypted, otherwise the encryption fails. Therefore, if an URL is encrypted into two different emails, the encryption in one email may be distinct from the encryption in the other email, but the URL (network address) itself is not unique. Moreover, the encryption does not prevent the embedding of previous links because the URL is the same in the previously encrypted link and the currently encrypted link. What is different is the encrypted data for the same URL. Thus, the Examiner's conclusion that the encrypted URL in Kim must be unique is erroneous.

Additionally, the alleged encryption has nothing to do with excluding generating network addresses that have not yet been accessed as recited in claim 25 and as argued by Appellants throughout the prosecution of the application. Therefore, the Examiner's point is irrelevant to the subject matter of claim 25. Accordingly, claim 25 distinguishes over Kim and Rienhoff.

For all of the reasons discussed above, it is respectfully submitted that the rejections are in error and that claims 1-22 and 25 are in condition for allowance. For all of the above reasons, Appellants respectfully request this Honorable Board to reverse the rejections of claims 1-22 and 25.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Stephen P. Catlin
Registration No. 36,101

JAO:KXH/add

Date: December 3, 2008

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to Deposit Account No. 24-0037
--